IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

IN RE PETITION OF INDEX NEWSPAPERS, LLC D/B/A THE STRANGER TO UNSEAL ELECTRONIC SURVEILLANCE DOCKETS, APPLICATIONS, AND ORDERS	MISC. CIVIL ACTION NO. 2:17-mc-00145 RSL **DECLARATION OF AARON D. MACKEY IN SUPPORT OF PETITION TO UNSEAL ELECTRONIC SURVEILLANCE DOCKETS, APPLICATIONS, AND ORDERS**

I, Aaron D. Mackey, declare as follows:

1. I am a staff attorney at the Electronic Frontier Foundation (EFF), a member-supported, non-profit civil liberties organization that works to protect free speech and privacy in the digital world. Founded in 1990, EFF now has more than 37,000 dues-paying members. EFF represents the interests of technology users in both court cases and broader policy debates surrounding the intersection of law and technology. I have been at EFF since September 2015. I am counsel (*pro hac vice* to be filed) for Petitioner Index Newspapers LLC d/b/a The Stranger in the above-captioned case. I am a member in good standing of the bar for the state of California, the District of Columbia, and am admitted to several federal courts. I have personal knowledge of the matters stated in this declaration.

DORSEY & WHITNEY LLP
COLUMBIA CENTER
701 FIFTH AVENUE, SUITE 6100
SEATTLE, WA 98104-7043
PHONE: (206) 903-8800
FAX: (206) 903-8820

2. The Petition filed by Index Newspapers LLC d/b/a The Stranger touches on a number of issues that EFF works on, including transparency, government surveillance, free speech, and privacy. Much of my work seeks to inform the public about government surveillance, including government requests for user data held by private companies such as Internet service providers (ISPs), telecommunications companies, social media platforms, and companies offering retail or other online services. I also regularly litigate cases under the Freedom of Information Act (FOIA) seeking access to records that document government surveillance.

3. Because these service providers collect and retain data about their users, the government often seeks such information via subpoenas, court orders to disclose stored communications records or install pen register / trap and trace (PR/TT) devices, search warrants, and other legal process. Many of the laws authorizing these demands allow law enforcement to place restrictions—either unilaterally or pursuant to court order—on what providers can say to their users and the general public about the requests they receive. As a result, users and the public often do not know the full extent of the government's demands for user data.

4. One of the most frequently used tools in these investigations are court orders issued under the Stored Communications Act (SCA), 18 U.S.C. § 2703(d), which authorize the government to obtain records of users' wire or electronic communications as well as the contents of older wire or electronic communications held in storage. *See* 18 U.S.C. § 2703(a)-(c).

5. Notably, in order to apply for a § 2703(d) order, the government need not demonstrate probable cause as it would in order to obtain a warrant. Instead, it must only "offer[] specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation." *Id.* § 2703(d).

6. In part because § 2703(d) orders do not meet the Fourth Amendment's standard for the issuance of warrants, EFF has long expressed concerns about the government's use of these

DORSEY & WHITNEY LLP
COLUMBIA CENTER
701 FIFTH AVENUE, SUITE 6100
SEATTLE, WA 98104-7043
PHONE: (206) 903-8800
FAX: (206) 903-8820

orders to obtain a range of sensitive and revealing information. In particular, EFF has advocated in the courts and Congress to require the government to seek a warrant to obtain the contents of communications, even where the SCA authorizes the use of a § 2703(d) order.[1] Although Congress has to date failed to amend the law, EFF's advocacy, particularly its *Who Has Your Back?* Report described below, has helped establish best practices for service providers to follow the Sixth Circuit's decision in *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010), and insist that the government rely on warrants rather than § 2703(d) orders when it seeks the contents of their users' communications.[2]

7. EFF has also called attention to the widespread use of § 2703(d) orders to obtain Cell Site Location Information (CSLI), which similarly has the potential to reveal extremely sensitive information about individuals' activities and associations.[3] This includes amicus efforts in the Supreme Court and federal appeals courts arguing that CSLI should be protected by the Fourth Amendment's warrant clause and therefore unavailable to the government using a § 2703(d) order.[4]

8. EFF seeks to bring transparency to requests for user data, in part by urging both private service providers and the government itself to make more information public.

9. Since 2011, EFF has conducted an annual survey called *Who Has Your Back*, in

---

[1] *See* Kevin Bankston, *Breaking News on EFF Victory: Appeals Court Holds that Email Privacy Protected by the Fourth Amendment*, EFF (Dec. 14, 201), https://www.eff.org/deeplinks/2010/12/breaking-news-eff-victory-appeals-court-holds.

[2] *See* EFF, *Who Has Your Back?* (July 2017), https://www.eff.org/who-has-your-back-2017. Notably, all twenty-six of the leading service providers evaluated in the most recent *Who Has Your Back?* Report require a warrant for content. *Id.*

[3] *See* Jennifer Lynch, *Federal Appellate Court Strikes Potential Death Blow to Privacy in New Cell Site Location Information Case*, EFF (May 31, 2016), https://www.eff.org/deeplinks/2016/05/graham-enbanc.

[4] Andrew Crocker & Jennifer Lynch, *Supreme Court Will Hear Significant Cell Phone Tracking Case*, EFF (June 5, 2017), https://www.eff.org/deeplinks/2017/06/supreme-court-will-hearsignificant-cell-phone-tracking-case.

DORSEY & WHITNEY LLP
COLUMBIA CENTER
701 FIFTH AVENUE, SUITE 6100
SEATTLE, WA 98104-7043
PHONE: (206) 903-8800
FAX: (206) 903-8820

which many providers are rated on, among other things, how they respond to government information demands for their customers' private information. EFF, *Who Has Your Back? Protecting Your Data from Government Requests*.[5] *Who Has Your Back* also awards stars to service providers that pledge to notify their users of all such demands made for customer data unless the provider is legally prohibited from doing so. This includes service providers, such as ISPs and phone companies, that are subject to PR/TT orders.

10. Thanks to consumer demand as well as EFF's work on *Who Has Your Back*, providers have adopted policies that are more protective of their users' information, consistent with applicable statutes and the Constitution. For example, it is now standard practice in the industry to insist that the government get a warrant before providers agree to turn over the contents of a customer account. It is also common for companies to publish "transparency reports," annual or semi-annual statements that describe the type and number of legal process the company has received in the most recent period and how the company responded. Leading companies including Amazon, Apple, Google, Facebook, and Microsoft, all publish regular transparency reports.

11. As a result of these developments, users are becoming more aware of when and how online service providers may release customer data in response to government demands.

12. EFF has also worked to end the government's practice of imposing indefinite nondisclosure orders or gags that prevent providers from disclosing that they have received demands for user data. Indefinite gags raise serious First Amendment concerns for providers and prevent the public from understanding the extent of government surveillance occurring in the United States.

13. EFF's work on gag orders includes representing two service providers, Credo Mobile, Inc. and Cloudflare, in a First Amendment challenge to the National Security Letter (NSL) statute, 18 U.S.C. § 2709. The NSL statute authorizes the FBI, without judicial oversight, to issue

[5] *Available at* https://www.eff.org/who-has-your-back-government-data-requests-2015.

DORSEY & WHITNEY LLP
COLUMBIA CENTER
701 FIFTH AVENUE, SUITE 6100
SEATTLE, WA 98104-7043
PHONE: (206) 903-8800
FAX: (206) 903-8820

subpoena-like demands for subscriber information with self-certified nondisclosure orders that prevent providers from even acknowledging the fact that they have received an NSL. *See Under Seal v. Sessions*, Nos. 16-16067, 16-16081, 16-16082 (9th Cir. 2017). Although these lawsuits began in 2011 and 2013 respectively, the government only recently modified certain nondisclosure orders in the cases, allowing Credo Mobile and Cloudflare to publicly identify that they had received NSLs. *See* Andrew Crocker, *Finally Revealed: Cloudflare Has Been Fighting NSL for Years*, EFF Deeplinks (Jan. 10, 2017).[6]

14. EFF has also supported companies, including Microsoft and Adobe, in fighting indefinite nondisclosure orders issued under a provision of the Stored Communications Act, 18 U.S.C. § 2705. *See* Andrew Crocker, *A Step Forward in Microsoft's Legal Battle for Transparency About Government Data Requests*, EFF Deeplinks (Feb. 17, 2017);[7] Andrew Crocker, *Adobe Puts an End to Indefinite Gag Order*, EFF Deeplinks (April 24, 2017).[8] A similar provision exists in the PR/TT statute, 18 U.S.C. § 3123(d).

15. Disclosure of the court records sought in The Stranger's Petition is in the public interest because it will provide information about the very types of legal demands for Internet and telephone subscriber data that, as described above, too often remain secret. Disclosure will also directly assist EFF's efforts to understand the extent of government demands for user information filed in this court.

16. Beginning in August 2017, I met and conferred telephonically and by email with the United States Attorney's Office for the Western District of Washington ("USAO") regarding the sealed judicial records that The Stranger seeks to access. On September 7, 2017, I provided a

---

[6] *Available at* https://www.eff.org/deeplinks/2017/01/finally-revealed-cloudflare-has-beenfighting-nsls-years.

[7] *Available at* https://www.eff.org/deeplinks/2017 /02/step-forward-microsofts-legal-battletransparency-about-government-data-requests.

[8] *Available at* https://www.eff.org/ deeplinks/201 7 /04/ ado be-puts-end-indefinite-gag-order.

DORSEY & WHITNEY LLP
COLUMBIA CENTER
701 FIFTH AVENUE, SUITE 6100
SEATTLE, WA 98104-7043
PHONE: (206) 903-8800
FAX: (206) 903-8820

draft of The Stranger's requested relief (proposed order) to the USAO. I discussed The Stranger's requested relief with the USAO during teleconferences on September 15 and October 13, 2017. No agreement was reached before the filing of the Petition.

17. Attached hereto as **Exhibit A** is a true and correct copy of a document titled "Report on the Use of Pen Registers and Trap and Trace Devices by the Law Enforcement Agencies/Offices of the Department of Justice for Calendar Year 2011," downloaded on November 14, 2017, at https://www.aclu.org/files/pdfs/privacy/DOJ_PRTT_FOIA/DOJ0975-RIF.pdf.

18. Attached hereto as **Exhibit B** is a true and correct copy of a document titled "Order and Notice to the Parties," Dkt. 22, in *In the Matter of the Application of Jason Leopold to Unseal Certain Electronic Surveillance Applications and Orders*, No. 13-mc-00712-BAH (D.D.C.).

19. Attached hereto as **Exhibit C** is a true and correct copy of a document titled "Order and Notice to the Parties," Dkt. 32, in *In the Matter of the Application of Jason Leopold to Unseal Certain Electronic Surveillance Applications and Orders*, No. 13-mc-00712-BAH (D.D.C.).

20. Attached hereto as **Exhibit D** is a true and correct copy of a document titled "Order and Notice to the Parties," Dkt. 37, in *In the Matter of the Application of Jason Leopold to Unseal Certain Electronic Surveillance Applications and Orders*, No. 13-mc-00712-BAH (D.D.C.).

21. Attached hereto as **Exhibit E** is a true and correct copy of a document titled "Google Transparency Report, Requests for User Information," downloaded on November 14, 2017, at https://transparencyreport.google.com/user-data/overview.

22. Attached hereto as **Exhibit F** is a true and correct copy of a Microsoft document titled "Law Enforcement Requests Report," downloaded on November 14, 2017, at https://www.microsoft.com/en-us/about/corporate-responsibility/lerr.

23. Attached hereto as **Exhibit G** is a true and correct copy of a document titled "Notice to the Parties," Dkt. 43, in *In the Matter of the Application of Jason Leopold to Unseal Certain*

DORSEY & WHITNEY LLP
COLUMBIA CENTER
701 FIFTH AVENUE, SUITE 6100
SEATTLE, WA 98104-7043
PHONE: (206) 903-8800
FAX: (206) 903-8820

Electronic Surveillance Applications and Orders, No. 13-mc-00712-BAH (D.D.C.).

24. Attached hereto as **Exhibit H** is a true and correct copy of Stephen W. Smith, *Gagged, Sealed & Delivered: Reforming ECPA's Secret Docket*, 6 Harvard L. & Policy Rev. 313-337 (2012), downloaded on November 14, 2017, at http://harvardlpr.com/wp-content/uploads/2013/06/Gagged-Sealed-and-Delivered.pdf.

25. Attached hereto as **Exhibit I** is a true and correct copy of a DOJ Memorandum dated October 19, 2017, titled "Policy Regarding Applications for Protective Orders Pursuant to 18 U.S.C. § 2705(b)," downloaded on November 14, 2017, at https://www.justice.gov/criminal-ccips/page/file/1005791/download.

26. Attached hereto as **Exhibit J** is a true and correct copy of Urs Gasser *et al.*, *Don't Panic: Making Progress on the "Going Dark" Debate* (2016), downloaded on November 14, 2017, at https://cyber.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf.

27. Attached hereto as **Exhibit K** is a true and correct copy of Nicole Hong, *Judge Questions Legal Authority to Force Apple to Unlock iPhones*, Wall St. J. (Oct. 26, 2015), downloaded on November 14, 2017, at https://blogs.wsj.com/law/2015/10/26/judge-questions-legal-authority-to-force-apple-to-unlock-iphones/.

28. Attached hereto as **Exhibit L** is a true and correct copy of Katie Benner and Eric Lichtblau, *U.S. Says It Has Unlocked iPhone Without Apple*, N.Y. Times (Mar. 28, 2016), downloaded on November 14, 2017, at https://www.nytimes.com/2016/03/29/technology/apple-iphone-fbi-justice-department-case.html.

29. Attached hereto as **Exhibit M** is a true and correct copy of a document titled "Government's Response to Petitioners' Supplemental Memoranda of Points and Authorities In Support of Their Application To Unseal Pen Register and/or Trap and Trace and Electronic Surveillance Applications, Orders, and Related Court Records," Dkt. 51, in *In the Matter of the*

DORSEY & WHITNEY LLP
COLUMBIA CENTER
701 FIFTH AVENUE, SUITE 6100
SEATTLE, WA 98104-7043
PHONE: (206) 903-8800
FAX: (206) 903-8820

Application of Jason Leopold to Unseal Certain Electronic Surveillance Applications and Orders, No. 13-mc-00712-BAH (D.D.C.).

30. Attached hereto as **Exhibit N** is a true and correct copy of a document titled "Joint Status Report," Dkt. 38, in *In re Petition of Jennifer Granick and Riana Pfefferkorn to Unseal Technical-Assistance Orders and Materials*, No. 16-mc-80206-KAW (N.D. Cal.).

31. Attached hereto as **Exhibit O** is a true and correct copy of Stephen Wm. Smith, *Kudzu in the Courthouse: Judgments Made in the Shade*, 3 Fed. Cts. L. Rev. 177 (2009), downloaded on November 14, 2017, at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2080279.

I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge.

Dated: November 15, 2017

By: *s/ Aaron D. Mackey*
Aaron D. Mackey

DORSEY & WHITNEY LLP
COLUMBIA CENTER
701 FIFTH AVENUE, SUITE 6100
SEATTLE, WA 98104-7043
PHONE: (206) 903-8800
FAX: (206) 903-8820